



August 2026

Submitted by:

Jeffery A. White

CEO & Founder

J.A. White & Associates, LLC



CMMC READINESS

Strengthening Cybersecurity Compliance
for Government Contractors



803-750-9150



info@jawwhite.com



www.jawwhite.com

As of August 2026, CMMC remains a critical cybersecurity requirement for the Defense Industrial Base, but there has been a significant change in implementation.

The Department of Defense suspended the planned rollout of CMMC Phase II (which would have required third-party assessments for many contractors beginning November 10, 2026) and launched a comprehensive review of the program. The DoD cited concerns over compliance costs, assessment capacity, and the burden on small businesses.

However, this **is not** a suspension of cybersecurity requirements:

- ✓ CMMC Phase I self-assessment requirements remain in effect for applicable contracts.
- ✓ Contractors must still comply with DFARS 252.204-7012, applicable NIST SP 800-171 security requirements, and other contractual cybersecurity obligations.
- ✓ Companies handling Controlled Unclassified Information (CUI) must continue implementing and documenting required cybersecurity controls.
- ✓ The DoD is reviewing the future structure of CMMC and may revise how compliance is verified, but contractors should continue preparing as though cybersecurity evidence and documentation will remain essential.

Why Organizations Choose J.A. White

